UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/686,547	10/14/2003	J. Scott Carr	P0869	3480

23735 7590 07/30/2007

DIGIMARC CORPORATION
9405 SW GEMINI DRIVE
BEAVERTON, OR 97008

EXAMINER	
HA, LEYNNA A	
ART UNIT	**PAPER NUMBER**
2135	
MAIL DATE	**DELIVERY MODE**
07/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/686,547	CARR ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 April 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51* is/are pending in the application.

4a) Of the above claim(s) *21-24 and 30-51* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20 and 25-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-51 are pending. Claims 21-24 and 30-51 withdrawn.

Claims 1-20 and 25-29 are examined. Claims 1, 12, and 25 are amended in amendment 4/30/2007.

Response to Arguments

2. Applicant's arguments with respect to claims 1-20 and 25-29 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-20 and 25-29 rejected under 35 U.S.C. 103(a) as being unpatentable over Sehr (US 6,999,936), and further in view of Wu, et al. (US 6,748,533).

As per claim 1:

Sehr discloses a method of verifying an age of a bearer of a document, said method comprising:

receiving first digital data corresponding to an age indicator, the first digital data being obtained from auxiliary data [*steganographically embedded*] in the document; **(col.10, lines 9-13)**

receiving second digital data corresponding to a biometric indictor, the second digital data being obtained from auxiliary data steganographically embedded in the document; **(col.6, lines 46-50 and col.11, lines 8-10)**

receiving third digital data corresponding to a biometric sample, wherein the biometric sample corresponds to the bearer; and **(col.7, lines 8-10 and col.13, lines 2-5)**

verifying the bearer's age when: i) the first digital data indicates that the bearer is at least as old as a predetermined age **(col.10, lines 13-15 and col.20, lines 22-27)**, and ii) the second digital data and the third digital data correspond. **(col.6 lines 53-55 and col.11, lines 19-22)**

Sehr discloses provides a document in the form of a card to gain access by verifying that the card data is authentic (col.2, lines 57-61). Sehr discloses retrieving and evaluating selected information recorded onto such documents. Sehr includes sets of information are in the forms of date of birth (DOB) or picture captured from a valid driver's license to determine the age (col.10, lines 10-13) and physical appearances or biometrics (co.11, lines 19-22 and col.33, lines 16-32). Sehr discloses encoded information can be scanned (col.22, lines 7-10) and communicated for comparison to the ones stored in the card (col.19, lines 24-30 and col.33, lines 32-45). Sehr discloses the encoding/decoding functions allow the related translation/conversion of information

with respect to different data formats and different data contents (col.7, lines 58-61 and col.20, lines 41-44). Although, Sehr teaches capturing biometric sample and storing the person's age and biometrics onto the card (col.11, lines 9-10 and col.13, lines 2-5), Sehr did not mention that these digital data being obtained from auxiliary data steganographically embedded in the document.

Wu discloses generating an invisible watermark and embedding the watermark on an article or document (col.3, lines 5-25 and col.6, lines 28-31). The claimed auxiliary data steganographically embedded in the document is in the form of a watermark embedded on the article, document, or passport because the watermark like auxiliary data steganographically embedded is invisible for protection against forgery (col.2, lines 45-48 and col.5, lines 14-33). having various portions of an article requiring protection against forgery or unauthorized modification (col.8, lines 51-54). Wu discloses embedding various information that includes identification portion in various portions of the document (col.7, lines 20-28). Wu gives an example depicting an article containing security information such as a passport where there are 3 portions. The first portion is marked with information that can be used to watermark one or more other portions include a first identification portion. The second portion includes another identification portion such as the name of the person. The third portion contains biometric data such as the person's fingerprint, personal particulars such as age and height and a third identification portion (col.7, line 5 – col.8, line 3). Wu discusses inputting facial image in a facial recognition engine (col.10, lines 53-67 and col.11, lines

5-13) and the authentication or verification process is carried out until all portions of the article are checked (col.9, lines 1-22).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Sehr with Wu to teach digital data being obtained from auxiliary data (watermark –Wu on col.2, lines 45-48 and col.5, lines 14-33) steganographically embedded in the document because invisibly embedded to protect against forgery so the authenticity of the document can be verified as legitimate (Wu on col.6, lines 18-32 and col.12, lines 48-53).

As per claim 2: **See Wu on col.6, lines 18-32 and col.12, lines 48-53;** discussing the method of claim 1, further comprising interrogating a data repository with the biometric indictor to obtain digital data being obtained from auxiliary data steganographically embedded in the document because

As per claim 3: **See Sehr on col.10, lines 13-15 and col.20, lines 22-27;** discussing the method of claim 2, further comprising interrogating the data repository with the age indictor to obtain the first digital information.

As per claim 4: **See Sehr on col.6, lines 46-50 and col.11, lines 8-10;** discussing the method of claim 2, wherein the second digital data comprises a biometric template associated with the bearer.

As per claim 5: **See Sehr on col.6, lines 46-50 and col.11, lines 8-10;** discussing the method of claim 4, wherein the biometric template includes information associated with at least one of the bearer's fingerprint, face map, hand geometry, iris, retina, DNA, voiceprint or vein pattern.

As per claim 6: **See Sehr on col.7, lines 13-31 and col.13, lines 1-4;** discussing the method of claim 1, wherein the third digital data is received through a network.

As per claim 7: **See Sehr on col.7, lines 13-31 and col.13, lines 1-4;** discussing the method of claim 6, wherein the network comprises the internet.

As per claim 8: **See Sehr on col.6, lines 46-50 and col.11, lines 8-10;** discussing the method of claim 1, wherein the biometric indicator comprises a biometric template.

As per claim 9: **See Sehr on col.6, lines 46-50 and col.11, lines 8-10;** discussing the method of claim 8, wherein the biometric template includes information associated with at least one of the bearer's fingerprint, face map, hand geometry, iris, retina, DNA, voiceprint or vein pattern.

As per claim 10: **See Wu on col.6, lines 29-31 and col.7, lines 23-25;** discussing the method of claim 1, wherein the third digital data further comprises a timestamp.

As per claim 11: **See Sehr on col.10, lines 13-15 and col.20, lines 22-27 and Wu on col.8, lines 1-3;** discussing the method of claim 4, wherein the auxiliary data comprises plural bits of data and wherein the biometric indicator and the age indicator comprise the same plural bits.

As per claim 12:

Sehr discloses a method of anonymously verifying an age or characteristic associated with a person, the person being in possession of an identification document, the identification document including a document layer and printing carried by the document layer, the identification document further including a digital watermark embedded therein, the digital watermark including a first set of information, the first set

of information including information to verify age or an age level of the person, said method:

receiving optical scan data corresponding to the identification document, the optical scan data being generated by an optical sensor; **(col.7, lines 8-10 and col.13, lines 2-5)**

decoding the scan data to obtain the first set of information **(col.7, lines 58-61 and col.20, lines 41-44)** [*included in the digital watermark, wherein the digital watermark is embedded*] in the identification document through hidden changes to data representing one or more items carried by the identification document; and **(col.6, lines 46-50 and col.11, lines 8-10)**

determining, based on the first set of information, the person's age or age level. **(col.10, lines 13-15 and col.20, lines 22-27)**

Sehr discloses provides a document in the form of a card to gain access by verifying that the card data is authentic (col.2, lines 57-61). Sehr discloses retrieving and evaluating selected information recorded onto such documents. Sehr includes sets of information are in the forms of date of birth (DOB) or picture captured from a valid driver's license to determine the age (col.10, lines 10-13) and physical appearances or biometrics (co.11, lines 19-22 and col.33, lines 16-32). Sehr discloses encoded information can be scanned (col.22, lines 7-10) and communicated for comparison to the ones stored in the card (col.19, lines 24-30 and col.33, lines 32-45). Sehr discloses the encoding/decoding functions allow the related translation/conversion of information with respect to different data formats and different data contents (col.7, lines 58-61 and

col.20, lines 41-44). Although, Sehr teaches capturing biometric sample and storing the person's age and biometrics onto the card (col.11, lines 9-10 and col.13, lines 2-5), Sehr did not mention that these digital data being obtained from auxiliary data steganographically embedded in the document.

Wu discloses generating an invisible watermark and embedding the watermark on an article or document (col.3, lines 5-25 and col.6, lines 28-31). The claimed auxiliary data steganographically embedded in the document is in the form of a watermark embedded on the article, document, or passport because the watermark like auxiliary data steganographically embedded is invisible for protection against forgery (col.2, lines 45-48 and col.5, lines 14-33). having various portions of an article requiring protection against forgery or unauthorized modification (col.8, lines 51-54). Wu discloses embedding various information that includes identification portion in various portions of the document (col.7, lines 20-28). Wu gives an example depicting an article containing security information such as a passport where there are 3 portions. The first portion is marked with information that can be used to watermark one or more other portions include a first identification portion. The second portion includes another identification portion such as the name of the person. The third portion contains biometric data such as the person's fingerprint, personal particulars such as age and height and a third identification portion (col.7, line 5 – col.8, line 3). Wu discusses inputting facial image in a facial recognition engine (col.10, lines 53-67 and col.11, lines 5-13) and the authentication or verification process is carried out until all portions of the article are checked (col.9, lines 1-22).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Sehr with Wu to teach digital data being obtained from auxiliary data (watermark –Sehr on col.2, lines 45-48 and col.5, lines 14-33) steganographically embedded in the document because invisibly embedded to protect against forgery so the authenticity of the document can be verified as legitimate (Sehr on col.6, lines 18-32 and col.12, lines 48-53).

As per claim 13: See Sehr on col.10, lines 13-15 and col.20, lines 22-27 and Wu on col.8, lines 1-3; discussing the method of claim 12, wherein the first set of information comprises at least one of the person's birth date, age level indicator or a concatenated string of data comprising the person's birth date and addition data.

As per claim 14: See Sehr on col.6, lines 46-50 and col.11, lines 8-10 and Wu on col.7, line 53 – col.8, line 3; discussing the method of claim 12, wherein the identification document further comprises a second set of information embedded therein, the second set of information corresponding to a third set of information that is printed on the identification document, wherein the second set of information comprises an index for accessing a data repository.

As per claim 15: See Wu on col.8, lines 22-30; discussing the method of claim 14, wherein the index comprises a hash of the third set of information that is printed on the identification document.

As per claim 16: See Sehr on col.7, lines 58-61 and col.20, lines 41-44 and Wu on col.8, lines 22-30;; discussing the method of claim 14, further comprising computing a hash of the third set of information that is printed on the identification document,

decoding the second set of information that is embedded in the identification document to obtain the embedded hash, and comparing the computed hash and the embedded hash to determine authenticity of the document.

As per claim 17: See Sehr on col.8, lines 1-15 and col.15, lines 10-19; discussing the method of claim 12, further comprising storing at least a portion of the first set of information in at least one of a list, electronic memory circuits and a data record, wherein the stored portion of the first set of information serves as an audit clue to evidence that the identification document has been examined.

As per claim 18: See Wu on col.11, lines 15-18 and see FIG.6; discussing the method of claim 17, wherein the first set of information comprises two or more random bits.

As per claim 19: See Sehr on col.7, lines 43-59 and col.15, lines 10-19; discussing the method of claim 18, wherein the first set of information comprises a date of birth.

As per claim 20: See Sehr on col.7, lines 43-59 and col.15, lines 10-19 and Wu on col.11, lines 15-18 and see FIG.6; discussing the method of claim 19, wherein a combination of the random bits and the date of birth decrease likelihood of overlapping birth dates, while maintaining an anonymous audit clue.

As per claim 25:

Sehr discloses a method comprising:

receiving optical scan data that is associated with an identification document, the identification document **(col.7, lines 8-12)** comprising *[plural-bits of steganographically*

embedded] in the identification document, wherein the *[plural-bits of steganographically embedded data]* comprise at least a first field and a second field, the first field carrying or linking to information corresponding to a bearer of the identification document **(col.6, lines 46-50 and col.11, lines 8-10)** and the second field corresponding to an age or age level of the bearer of the identification document; **(col.10, lines 13-15)**

receiving information carried by the document, separate from the data corresponding to at least the second field- and generating a reduced-bit representation of the received information; and **(col.5, lines 1-10 and col.10, line 1-12)**

comparing data corresponding to the second field with the reduced-bit representation to verify an age level of the document. **(col.33, lines 10-30 and col.20, lines 22-27)**

Sehr discloses provides a document in the form of a card to gain access by verifying that the card data is authentic (col.2, lines 57-61). Sehr discloses retrieving and evaluating selected information recorded onto such documents. Sehr includes sets of information are in the forms of date of birth (DOB) or picture captured from a valid driver's license to determine the age (col.10, lines 10-13) and physical appearances or biometrics (co.11, lines 19-22 and col.33, lines 16-32). Sehr discloses encoded information can be scanned (col.22, lines 7-10) and communicated for comparison to the ones stored in the card (col.19, lines 24-30 and col.33, lines 32-45). Sehr discloses the encoding/decoding functions allow the related translation/conversion of information with respect to different data formats and different data contents (col.7, lines 58-61 and col.20, lines 41-44). Although, Sehr teaches capturing biometric sample and storing the

person's age and biometrics onto the card (col.11, lines 9-10 and col.13, lines 2-5), Sehr did not mention that these digital data being obtained from auxiliary data steganographically embedded in the document.

Wu discloses generating an invisible watermark and embedding the watermark on an article or document (col.3, lines 5-25 and col.6, lines 28-31). The claimed auxiliary data steganographically embedded in the document is in the form of a watermark embedded on the article, document, or passport because the watermark like auxiliary data steganographically embedded is invisible for protection against forgery (col.2, lines 45-48 and col.5, lines 14-33). having various portions of an article requiring protection against forgery or unauthorized modification (col.8, lines 51-54). Wu discloses embedding various information that includes identification portion in various portions of the document (col.7, lines 20-28). Wu gives an example depicting an article containing security information such as a passport where there are 3 portions. The first portion is marked with information that can be used to watermark one or more other portions include a first identification portion. The second portion includes another identification portion such as the name of the person. The third portion contains biometric data such as the person's fingerprint, personal particulars such as age and height and a third identification portion (col.7, line 5 – col.8, line 3). Wu discusses inputting facial image in a facial recognition engine (col.10, lines 53-67 and col.11, lines 5-13) and the authentication or verification process is carried out until all portions of the article are checked (col.9, lines 1-22).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine Sehr with Wu to teach digital data being obtained from auxiliary data (watermark –Sehr on col.2, lines 45-48 and col.5, lines 14-33) steganographically embedded in the document because invisibly embedded to protect against forgery so the authenticity of the document can be verified as legitimate (Sehr on col.6, lines 18-32 and col.12, lines 48-53).

As per claim 26: See Sehr on col.33, lines 10-30 and col.20, lines 22-27; discussing the method of claim 25, wherein the data corresponding to the second field does not betray the identity of the authorized bearer of the identification document.

As per claim 27: See Sehr on col.11, lines 16-22 and col.13, lines 1-5; discussing the method of claim 26, further comprising storing the data corresponding to the second field in a data repository to evidence examination of the identification document.

As per claim 28: See Sehr on col.30, lines 24-27 and Wu on col.8, lines 63-67; discussing the method of claim 26, further comprising printing the data corresponding to the second field to evidence examination of the identification document.

As per claim 29: See Sehr on col.7, lines 58-61 and col.20, lines 41-44; discussing the method of claim 25, wherein said receiving information carried by the document comprises receiving data corresponding to at least one of data generated by a barcode scanner, optical character recognizer, manual entry or watermark decoder.

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100